Security requirements, risks and recommendations for small enterprise and home-office environments

D. Spinellis
Department of Information and Communication Systems, University of the Aegean, Karlobasi, Greece
S. Kokolakis
Department of Informatics, Athens University of Economics and Business (AUEB), Athens, Greece
S. Gritzalis
Department of Information and Communication Systems, University of the Aegean, Karlobasi, Greece

Keywords
Risk, Risk management, Small firms, Security, Recommendations

Abstract
The pervasive use of information technology in enterprises of every size and the emergence of widely deployed ubiquitous networking technologies have brought with them a widening need for security. Information system security policy development must begin with a thorough analysis of sensitivity and criticality. Risk analysis methodologies, like CRAMM, provide the ability to analyse and manage the associated risks. By performing a risk analysis on a typical small enterprise and a home-office set-up the article identifies the risks associated with availability, confidentiality, and integrity requirements. Although both environments share weaknesses and security requirements with larger enterprises, the risk management approaches required are different in nature and scale. Their implementation requires co-operation between end users, network service providers, and software vendors.

Information Management & Computer Security
7/3 [1999] 121–128
© MCB University Press
[ISSN 0968-5227]

Introduction

Advances in networking technology, the explosive growth of the Internet, and the liberalisation of telecommunication markets increasingly allow small businesses and private individuals to reap the benefits of sophisticated networked computer applications. Examples of such applications include electronic commerce, teleworking, multimedia communication, information access, and entertainment. Unfortunately, the realisation of these applications is often hampered by insecurities typical of open networks: messages can be intercepted and manipulated, the validity of documents can be denied, and personal data can be illicitly collected. Large enterprises can typically design and implement security policies for their data networks (Kabay, 1996) and implement them using technologies such as virtual private networks and firewalls. However, the use of networked information systems within small enterprises and modern home-office environments can be the source of serious security problems, because such enterprises typically lack the technical expertise and resources to create and maintain a suitable level of security.

The adoption of a systematic approach and a standard methodology for the establishment of a baseline on security practices for the emerging ubiquitous networking environment allows the stakeholders of this environment (users, network service providers, equipment and software vendors) to evaluate the required security level and take appropriate strategic and tactical decisions.

Risk analysis, an orderly process adapted from practices in management, is a valuable methodology for every attempt towards the establishment of a secure information system (IS), as it addresses two important issues (Eloff *et al.*, 1993):

1. The need for a systematic method to identify information technology (IT)-related risks. Continuous technological evolution, IS complexity, diversity in applications, technologies, and configurations are some of the reasons why identifying and assessing risks is considered such a laborious task.
2. Total security is not feasible. In addition, an enterprise must justify expenditures for security. This brings out the need for a method to improve the basis for decisions; one can thus select a set of safeguards that will provide a level of security analogous to the level of risk in a cost-effective manner.

In this paper we apply a risk analysis methodology to representative examples of the emerging ubiquitous networking environment, analyse the associated risks, and provide an overview of approaches for risk management. The paper can serve as a rough roadmap marking the areas where the peculiarities of the new environment require novel approaches from end users, vendors, and network service providers.

Risk analysis and management methodologies

One cannot reasonably develop security policies and procedures without clearly understanding the systems that must be protected and how valuable they are to the enterprise. In addition, one must determine the probability that the assets will be threatened. Therefore, the objective of risk analysis is to identify and assess the risks to which the IS and its assets are exposed in order to select appropriate and justified security safeguards. The analysis of risks is performed in five stages (ISO/IEC/JTC1, 1996):

1. asset identification and valuation;
2. threats assessment;

The current issue and full text archive of this journal is available at
http://www.emerald-library.com

3 vulnerabilities assessment;
4 existing/planned safeguards assessment; and
5 risk assessment.

Assets are the elements of an IS that possess a value. A security incident that will affect an asset will also have an impact on the owner of the asset (i.e. the organisation, the enterprise, or the individual). Assets are evaluated according to the impact of a probable asset impairment. Threats need to exploit a certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk an IS is exposed to. The implied conceptual model (CEC, 1993a) is given in Figure 1.

The risk analysis methods database developed within the CEC/INFOSEC Programme (CEC, 1993b) contains more than 70 risk analysis methods. In our analysis we chose CRAMM, the United Kingdom Central Computer and Telecommunication Agency's (CCTA) Risk Analysis and Management Method, for the following reasons:

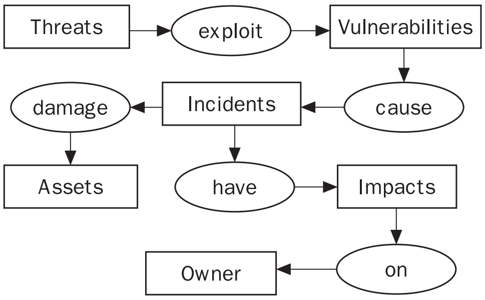
1 CRAMM has been extensively used since 1987, and is considered an effective and reliable method;
2 as CRAMM is the mandatory security analysis method for UK governmental organisations it has been thoroughly tested; and
3 CRAMM is supported by a software tool.

The CRAMM software tool provides automated selection of countermeasures. CRAMM countermeasures are also ascribed to policy statements that constitute the security requirements of the system and form the basis for the development of a security policy.

The CRAMM methodology (UKCCTA, 1996) involves three stages:

1 *Asset identification and assessment*. This requires the development of a complete model of the IS and considers both tangible assets (e.g. IT equipment) and intangible assets (e.g. information). The asset assessment follows a quantitative approach based on a numeric scale ranging from 1 to 10. The value of an asset is analogous to the impact of the destruction, unavailability, disclosure, or modification of the asset.
2 *Threats and vulnerabilities identification and assessment*. This is achieved by means of using predefined questionnaires. The overall risk is estimated as a combination of the triple effects of threats/vulnerabilities, impacts and asset values.
3 *Countermeasure selection*. This task is performed automatically by the software tool. The CRAMM tool, however, allows for expert intervention and refinement. CRAMM also facilitates the development of a security policy, the identification of roles and assignment of responsibilities to roles, and the monitoring of countermeasure implementation.

Figure 1
Threats, assets and related concepts



Scenario description

Our study has been based on two exemplary scenarios. The first one concerns a small enterprise and the second a home user that maintains a home-office environment.

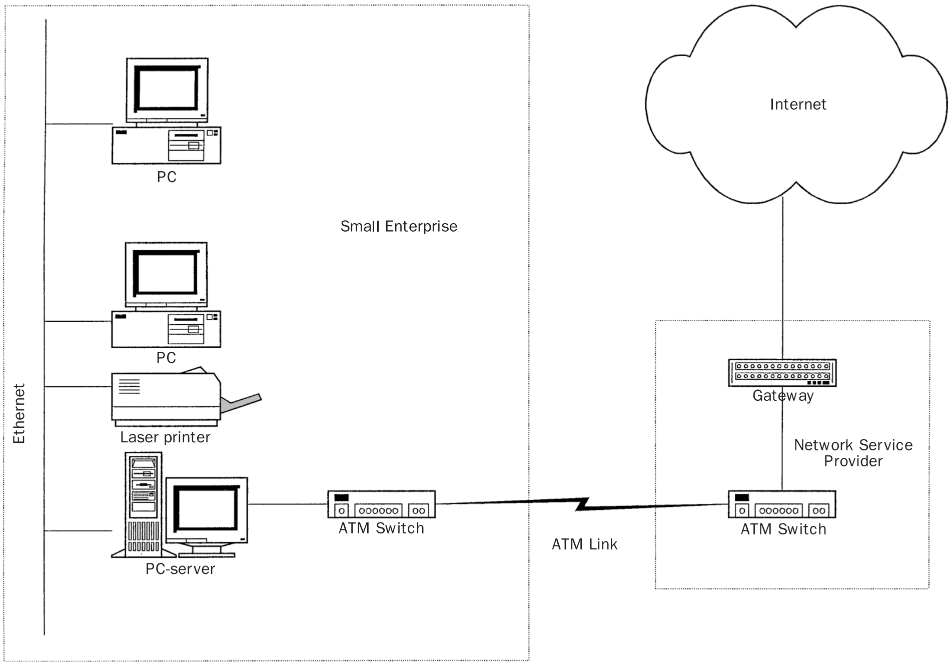
Small enterprise

The first scenario represents a modern small enterprise that makes use of advanced networking technology, while retaining a basic computing infrastructure. The infrastructure of the enterprise includes three PCs and a printer connected via an ethernet local network. Two of the PCs are used as workstations, whilst the third one is used as a server. The latter also hosts a Web server. An ATM line connects the enterprise with a network service provider that provides Internet connectivity (Figure 2).

The business functions of the enterprise that involve the use of computing facilities are the following:

- *Sales* – this involves the process and storage of client-related data including personal client information, orders, and a record of past transactions.
- *E-commerce* – commercial transactions over the Internet. It includes the provision of product information and price lists, electronic payment, and EDI applications. The enterprise maintains a Web server for accepting online orders and providing product and corporate information.
- *Administration* – the handling of administrative data such as letters, contracts, personnel data, and other documents.

Figure 2
Small enterprises



- *Finance* – the processing of financial data, such as invoices, taxation data, and cost statements.
- *Electronic communication* – this includes e-mail, audiovisual communication, and Web browsing.

Home-office environment

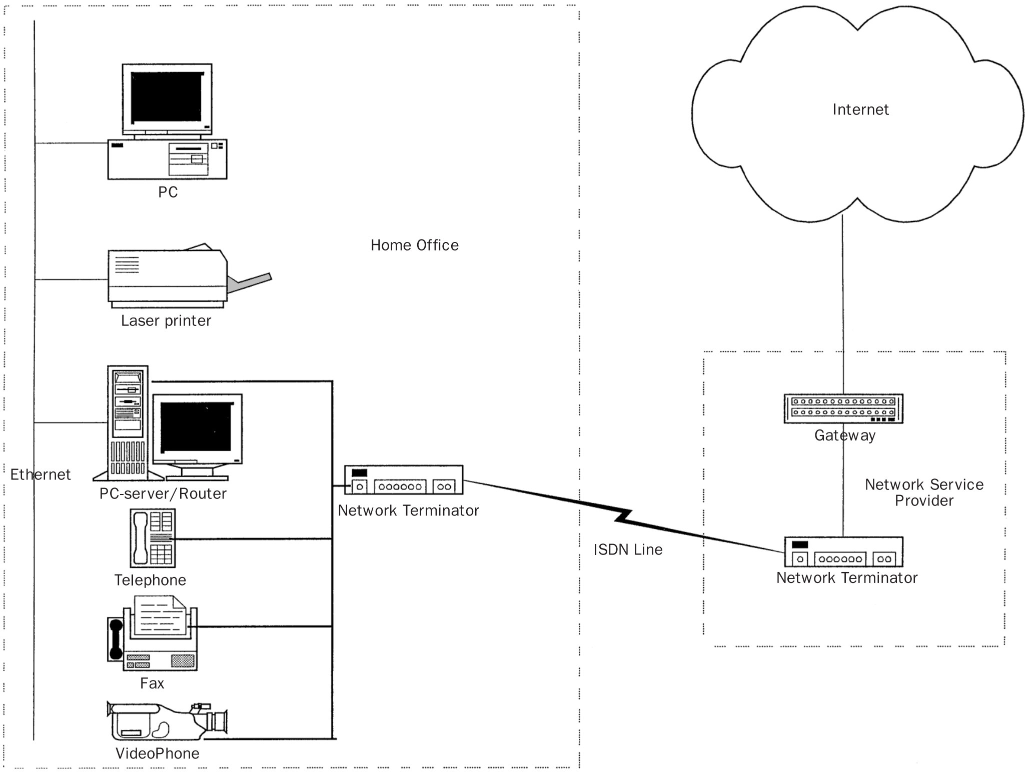
The second scenario represents the case of a home user who uses ISDN technology for both entertainment and business purposes (Figure 3). The equipment used includes two PCs and a printer connected to a local ethernet network and through an ISDN line to a network service provider who provides Internet connectivity. The ISDN line gives the user the ability to use the same connection for a video phone, a fax, and a conventional telephone. The basic activities in this set-up include:

- *Electronic communication* – this includes e-mail, audio-visual communication, and Web browsing.
- *Processing of electronic documents* – document processing through office automation tools. It involves multimedia, hypertext, spreadsheet and word processing documents. These documents may be an essential resource for the professional activities of the user.
- *Infotainment* – Entertainment through information networks. This can include activities such as Web browsing, multi-user game playing, participation in virtual environments, and the delivery of multimedia data.

Risk analysis

After performing a risk analysis of the two scenarios using the outlined methodology, we found that, although different in size, the small enterprise and the home-office face a similar level of risk. This can be justified if we consider the risk analysis process. Risk is calculated as a combination of the value of assets (estimated according to the impact an asset impairment may have), the level of threat, and the level of vulnerability. The threats are common in both cases and result mainly from the use of open, high speed networks, though physical threats (e.g. fire) have not been ignored. The level of vulnerability is similar in both cases with the home-office case being more vulnerable because of the use of the same facilities for both work and entertainment. The only significant differences have been identified through impact assessment, where it appears that the small enterprise has a greater need for availability, confidentiality and integrity for the purpose of conducting electronic commerce (Warren and Furnell, 1998). However, the home-office also requires a high level of protection since all professional activities are conducted through the same computing facilities. The following paragraphs provide an overview of the availability,

Figure 3
Home-office environment



confidentiality, and integrity requirements that we identified.

Availability

Large enterprises may have several computing installations and produce a wide range of products, so the unavailability of a certain installation can be overcome by activating other resources. In contrast to large enterprises, home-offices and small enterprises have a greater dependency on their IT systems since their owners typically have no other source of income or spare IT resources.

Confidentiality

Unauthorised disclosure of information is a significant threat in both scenarios. Especially in the case of a small enterprise, electronic commerce data exchanged are quite sensitive (e.g. credit card numbers) and often protected by law. In addition, it is important to protect the privacy of the employees of the small enterprise, the home user, and their clients.

Integrity

Integrity issues are quite important especially considering the application of electronic commerce. Modification of e-commerce data may result in high financial losses. A wide range of potential perpetrators may be interested in deliberately modifying financial, commercial, and EDI data. These may be dissatisfied or malevolent customers, lunatics, or aggressive competitors.

Tables I and II show the highest risk values in the two case scenarios. The evaluation of risks follows a scale of 0-7 where 6 and 7 mostly apply to safety critical systems. CRAMM estimates risk values for every combination of asset impact, threat, and vulnerability. The list of all risks is several pages long and is considered beyond the scope of this paper.

Risk analysis conclusions

The main conclusions resulting from our risk analysis review are the following:

- Small enterprises and home-offices face risks of the same kind and of a similar level.
- PC-based systems have not been designed for professional use in open environments and consequently do not offer adequate security services. This makes these systems quite vulnerable.
- Both cases are associated with a high risk level, similar to the risk level of large enterprises. It is not the size that counts, but the nature of activities performed and the threat environment. Professional and commercial activities always show a great

dependency on availability, confidentiality and integrity of information, and computer technology services and data. Though in absolute monetary values the assets may not seem important, if one considers the financial ability of their owners the significance of these assets becomes apparent. Moreover, the threats encountered are the same as with those of large enterprises. This is the result of the use of high speed, public networks, and in particular the Internet.

The aforementioned conclusions highlight the necessity for risk management. This is performed by determining the security requirements and selecting appropriate countermeasures.

Risk management

Managing risks may follow three strategies: risk reduction, risk transfer, and risk acceptance. Accepting risk means that although one is aware of it one prefers to accept the consequences instead of applying countermeasures. This applies in the case where the cost of countermeasures is significantly higher than the impact of a potential security breach. An example of risk transfer is insurance and applies in particular to physical assets (e.g. computers). Note that in most cases the insurance contract covers the replacement value of equipment and not the value of the data contained or processed by it. Finally, reducing risk could be achieved by means of reducing threat, reducing vulnerability, reducing impact, or recovering from threat occurrences.

Table I
Availability-related risk values (scale 0-7)

	15M	1H	3H	12H	1D	2D	1W	2W	1M	2M
Small enterprise	1	2	2	3	3	3	4	4	5	5
Home-office	–	–	2	2	2	3	3	4	4	4

Notes: Unavailability: 15M = 15 min.; 1H = 1 hour; 3H = 3 hours; 12H = 12 hours; 1D = 1 day; 2D = 2 days; 1W = 1 week; 2W = 2 weeks; 1M = 1 month; 2M = 2 months

Table II
Integrity- and confidentiality-related risk values (scale 0-7)

	B	T	O	SE	WE	DM	In	Or	Rc	Nd	Mr	Tm
Small enterprise	4	5	4	3	4	5	3	3	3	3	2	1
Home-office	4	5	4	2	3	4	4	4	4	4	3	3

Notes: B = loss of data since last back-up; T = total loss of data;
O = disclosure to outsiders; SE = small-scale errors; WE = widespread errors;
DM = deliberate modification; In = insertion of false message;
Or = repudiation of origin; Rc = repudiation of receipt; Nd = non-delivery;
Mr = mis-routeing; Tm = traffic monitoring

CRAMM provides a list of recommended countermeasures that reduce risk in any of the ways mentioned above. A security expert may select those that provide the highest effectiveness with the lowest cost. As a result of the high risk values that we identified in the previous section, we compiled a lengthy list (a few hundred items) of requirements (Dubois and Wu, 1996; Rohm *et al.*, 1998) and countermeasures to be applied. The most important requirements are abstracted in Table III. The cost of implementing the countermeasures is obviously beyond the abilities not only of a home-office environment, but also of a small enterprise.

Considering the lack of resources, the lack of security provisions in PC-based systems, and the currently low security level of Internet technologies, there is no way a small enterprise or home user can afford an adequate level of security today. It is thus necessary to advance the state of the art to provide a secure baseline for small enterprises and home users. This will involve vendors, network service providers, government, and private organisations.

System software vendors

Security services (e.g. authentication, discretionary access control, etc.) should be incorporated into PC operating system software. However, if these offer a wide range of security options it is obvious that a non-expert will be puzzled. Therefore, specific "security profiles" could be offered so that the user can select the profile that is closest to their needs. When selecting a profile the corresponding security policy will be automatically employed.

Network service providers

They may offer a wide range of security services, such as anonymity, encryption, back-up, incident reporting, and data recovery services. Many of these services can be provided with minimal user intervention if they are standardised and tightly integrated with the networking software.

Third parties

It is absolutely essential to develop and deploy a security infrastructure (including a Public Key Infrastructure (PKI)) that will address the needs of small enterprises. In addition, a network of accredited certifiers (Wilsher and Kurth, 1996) that will provide security certification services for PC software products would absolve users from difficult-to-perform security tests of off-the-shelf software products. Additionally, non-expert users will benefit from "security

Table III
Risk analysis requirement specifications and possible solutions

Requirement	Possible solution
User IDs – All users should be allocated an identifier (user ID)	The operating system should ensure that access is only granted with the provision of an ID and a means of authentication (e.g. password, smart card)
Password management – Passwords should be difficult to guess. They should be kept in a one-way encryption form; they should change at least once every six months; they should be transmitted in an encrypted form; they are not to be stored in macros or function keys	Current practice in PC-based systems does not comply with the above requirements (e.g. passwords are often stored in macros to be used for ftp or telnet sessions). The problem could be addressed by means of using proactive password checkers, password generators and the provision of relevant services by the operating system. Smart cards provide an alternative authentication method, but appropriate infrastructure is needed (e.g. inexpensive and easy-to-use cards readers, standardisation in smart card technology)
Logical access control – The owner of a file or a program should be provided with the facility to specify who is allowed to access the file or program (discretionary access control). All files and directories should have an owner	Incorporate discretionary access control in PC-based operating systems and networking software
Access control – access rights should be reviewed at regular intervals. Inactive accounts should be locked	Automate the review of access rights based on checklists and procedure available in certified security handbooks
Auditing tool – a range of facilities for keeping and analysing audit logs should be provided. Audit logs should be available in database format and reports should be provided in word-processing format	Provision of easy-to-use audit tools, with predefined auditing profiles and customisation options. Quite often the difficulties of managing huge audit logs force users not to activate auditing
Investigation of incidents – when incidents are detected or suspected they must be investigated in a thorough manner	Development of incident reporting schemes (IRS). General purpose CERTs will not be able to address the increasing needs for incident response in the future. The development of sector-specific IRS appears as a more promising solution
System security acceptance criteria – acceptance criteria should be established against which suitable tests should be carried out prior to acceptance of a system as providing the required level of security	Certification of software by accredited certifiers
Software integrity checks – breaches of software integrity should be detected and prevented	Several security packages offer file integrity checking. These facilities could be integrated into the operating system
Detection of malicious software – any malicious software should be detected, identified, isolated and removed. Users have to deal with attacks from malicious network applets which can cause many problems, such as denial of service, invasion of privacy, and annoyance	Anti-virus tools and good practice rules. All anti-virus tools must be kept up to date. Digital signature techniques can be used for the verification of signed applets (e.g. Microsoft's authenticode technology) (Gritzalis *et al.*, 1999)
Security of network services – the service provider's contract should formally define the security issues for the network service	Standard contracts and terms of business relating to security issues can be standardised by relevant bodies and applied uniformly across all network service providers
Mutual authentication – all communicating entities should be authenticated	Public-key infrastructure (PKI); application of cryptographic and authentication protocols for implementing virtual private networks

(continued)

Table III

Requirement	Possible solution
Network access – the flow of traffic to and from external networks should be controlled	Integrate firewall functionality and auditing facilities into router and gateway software
Message origin authentication – the origin of a message should be authenticated	Research has provided several non-repudiation techniques that need to be standardised and employed. Digital signatures, based on public-key cryptography, are widely considered as crucial. Legal and regulatory issues have to be addressed by governments leading towards an integrated framework for secure network transactions
Operational change procedures – management responsibilities and associated procedures are necessary to ensure satisfactory control of all changes to equipment, software and procedures	Minimise the security vulnerabilities that can be introduced by user modifications. Encourage the use of certified security handbooks and checklists
Operating system changes – when such changes occur the security of the system should be reviewed to ensure that the changes have not introduced any adverse effects	Include security checks in the installation procedures of operating systems updates. Provide a certification framework for operating system upgrade procedures
Access to manager accounts – the system administrator account should be used for day-to-day operations	Design network and operating system administration procedures to minimise the need for a system administrator account
Data back-ups – Back-ups should be taken of all essential business data; back-up should be stored in a separate location; it should be possible to recreate data lost since the last back-up	Provision of back-up services by network service providers; for example, user data back-up can be performed over a high-speed network
Security awareness – staff should be aware of IT security issues	Small enterprises cannot afford seminars and training programmes on security, but at least users should be aware of the threats and of the basic security requirements
Security policies – an IT security policy should be documented	Use of baseline or standard security policies developed by associations, standardisation bodies and other trusted organisations
Incident handling – security incidents should be detected and investigated thoroughly	Development of sector-specific incident reporting schemes. Some types of incidents could be automatically reported and managed by the network service providers

handbooks” that will contain security policies, security procedures and checklists.

Users

In most cases measures that transfer risk or enable recovery from security incidents require fewer resources and are easier to apply. Two measures of this kind, insurance and back-up, have always provided a good level of security. Insurance may cover losses in equipment and back-up data losses. Back-up data should have the same protection as active data, should be stored in a different location, and the restore procedure should be tested and be known by all users. Given a security infrastructure, the emerging network technologies could allow WAN-based back-up services to be provided. Passwords are thought to be the weakest point of attack in almost every system. Good password management practices provide a highly important defence safeguard in an IT system.

Conclusions

The advent of the Information Society brings up new business opportunities for small and medium-size enterprises (SMEs) and promotes new forms of work organisation. Moreover, growth and employment largely depend on the proliferation of teleworking and the use of telematic services by SMEs (Bangemann Committee, 1994).

The risk analysis review performed for the purposes of this paper has shown that small enterprises and home offices currently operate in a high risk environment. In addition, current security infrastructure and business practices do not allow for effective risk management. Consequently, the lack of a secure environment for small enterprises and home offices can be expected to hinder their development. Moreover, recent security surveys (Hinde, 1998) show that the rate of security breaches has increased in the last few years. The latest survey conducted by the UK Audit Commission reports that 45 per cent of organisations surveyed had suffered from computer fraud and abuse – up from 36 per cent three years ago (UK Audit Commission, 1998).

This paper provides a rough roadmap for the establishment of a secure environment for small enterprises and home offices. The proposed solutions are based on novel approaches to security management practices, and imaginative use of sophisticated technologies. Their deployment requires tight co-operation between all stakeholders in the emerging network infrastructure: end users, network service providers, and software vendors.

References

Bangemann Committee (1994), *Europe and the Global Information Society: Report of the High Level Group on the Information Society (Bangemann Report)*, Commission of the EU, Brussels.

Commission of the European Communities (1993a), Glossary of information systems security, DGXIII, INFOSEC Programme/ S2001.

Commission of the European Communities (1993b), Risk analysis methods database, DGXIII, INFOSEC Programme/S2014/WP08.

Dubois, E. and Wu, S. (1996), "A framework for dealing with and specifying security requirements in information systems", in Katsikas, S.K. and Gritzalis, D. (Eds), *Information Systems Security: Facing the Information Society of the 21st Century*, Chapman-Hall, pp. 88-99.

Eloff, H.P., Labuschagne, L. and Badenhorst, K.P. (1993), "A comparative framework for risk analysis methods", *Computers and Security*, Vol. 12 No. 6, pp. 597-603.

Gritzalis, S., Aggelis, G. and Spinellis, D. (1999), "Architectures for secure portable executable content", *Internet Research Journal*, Vol. 9 No. 1, pp. 16-24.

Hinde, S. (1998), "Recent security surveys", *Computers and Security*, Vol. 17 No. 3, pp. 207-10.

ISO/IEC/JTC1 (1996), *Information Technology – Security Techniques – Guidelines for the Management of IT Security, GMITS*, ISO/IEC DTR13335.

Kaba, E. (1996), *The NCSA Guide to Enterprise Security: Protecting Information Assets*, McGraw-Hill.

Rohm, A., Pernul, G. and Herrmann, G. (1998), "Modelling secure and fair electronic commerce", *Proceedings of the 14th Annual Computer Security Applications Conference*, IEEE Computer Press, pp. 155-64.

UK Audit Commission (1998), *Ghost in the Machine – An Analysis of IT Fraud and Abuse*, The Audit Commission, UK.

United Kingdom Central Computer and Telecommunication Agency (1996), *CCTA Risk Analysis and Management Method: User Manual*, version 3.0 edition, HMSO, London.

Warren, M.J. and Furnell, S.M. (1998), "Electronic commerce: winners and losers", *Proceedings of the INC'98 1st International Network Conference*, University of Plymouth, pp. 197-202.

Wilsher, R.G. and Kurth, H. (1996), "Security assurance in information systems", in Katsikas, S.K. and Gritzalis, D. (Eds), *Information Systems Security: Facing the Information Society of the 21st Century*, Chapman-Hall, pp. 74-87.